一种车载mesh网络漫游匿名接入认证协议

吴修强[1] 马 华[1] 张卫东[2] 裴庆祺[2]
(西安电子科技大学理学院 西安 710071)[1]
(西安电子科技大学计算网络与信息安全教育部重点实验室 西安 710071)[2]

摘 要 无线mesh网络的特性使它面临着比传统无线网络更大的安全挑战。其安全解决方案必须兼顾安全性和应用环境等因素。用户节点的接入认证与密钥协商是节点漫游时最基本的安全协议,是安全路由等协议的实现基础。在多跳车载mesh网络用户节点接入认证中,用户身份信息的保护非常重要,然而有关车载mesh网络用户节点漫游时的匿名认证的研究较少,为此,在充分考虑无线mesh网络自身特点的基础上,结合基于Hash和Diffie-Hellman算法,提出一种高效的用户节点匿名接入认证与密钥协商协议。分析发现,该协议不仅可以满足安全性需求,在现实应用中也是可行的。

关键词 mesh,漫游,匿名认证,协议,隐私保护

Efficient Roaming Authentication with Anonymity Protocol for Wireless Vehicle Mesh Networks

WU Xiu-qiang[1] MA Hua[1] ZHANG Wei-dong[2] PEI Qing-qi[2]
(School of Science, Xidian University, Xi'an 710071, China)[1]
(Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071, China)[2]

Abstract Due to their own characteristics, wireless mesh networks are facing more security challenges than traditional networks. Their security mechanism should take into account both the security and the application environment. Anonymous authentication and key negotiation, when users roam, are an elementary protocol in constructing a secure network system, and are the implementation foundation of the secure routing protocol. The user's certificated in wireless mesh networks, protection of identity information is very important, but the study of anonymous authentication and key negotiation when users roam in wireless mesh networks was too little. Motivated by these concerns, on the enough consideration on the attack methods for wireless networks and the characteristics of wireless mesh networks, an efficient roaming authentication with anonymity protocol for wireless vehicle mesh networks was proposed, in which the ID based public key cryptography and Diffie-Hellman algorithm were adopted. Analysis shows that this protocol can be used to guarantee the security of wireless mesh networks, and at the same time, it can meet the special application environment of wireless vehicle mesh networks.

Keywords Mesh, Roaming, Anonymous authentication, Protocols, Privacy protection

1 引言

无线mesh网络即"无线蜂窝网格网络",是基于IP协议的无线宽带接入技术,是Internet的无线版本。一般认为,WMN是一种由无线链路连接路由器和终端设备的无线网络,融合了WLAN和Ad hoc网络的优势,具有快速部署和易于安装、非视距传输、健壮性、结构灵活、高带宽等特点,支持多点对多点的网状结构。在无线mesh网络中,任何无线设备节点都可同时作为路由器或AP,网络中的每个节点都能发送和接收信号,每个节点都能与一个或多个对等节点进行直接通信。各用户节点可以通过相邻的其他用户节点,以多跳的方式实现到骨干网的连接,新用户可以通过它周围的其他用户节点很方便地接入到网络中。从某种意义上讲,mesh网络更主要是一种网络架构思想,主要功能体现在无中心、自组网、多级跳接和路由判断选择等。mesh网络拓扑特征是网络中只有一个或多个节点充当网关节点接入基础设施网络,其他节点通过相邻节点中继连接到网关,再接入到互联网。目前研究者主要关注的无线mesh网络分为3种拓扑结构:平面结构、多级结构、混合结构。国内外研究比较多的是混合网络结构[3,6]。无线网状结构作为可以解决"最后1km"网络接入瓶颈问题的方案,已被写入IEEE 802.16 (WiMax)无线宽带接入网络标准中,被纳入IEEE 802.11s mesh标准草案中。从技术特点来看,WMN将成为未来无线城域网(WMAN)核心网理想的组网方式,极有可能挑战3G技术,成为构建B3G/4G的潜在技术之一,同时是迄今为止唯一一种建设商用移动Ad hoc网络的可行技术[7]。

到稿日期:2009-03-30 返修日期:2009-07-06 本文受国家自然科学基金(60803151)资助。
吴修强 硕士生,主要研究方向为网络与信息安全,E-mail:xiuqiangwu@163.com;马 华 教授,主要研究方向为网络与信息安全、密码学;张卫东 高级工程师,主要研究方向为网络与信息安全;裴庆祺 博士,副教授,主要研究方向为计算机安全、无线传感器网络安全。

无线 mesh 网络在具有以上优势的同时也存在很多的问题，如异构性、通信延迟、安全等。尤其是安全问题是影响 mesh 网络技术推广应用的主要原因。相对于有线网络来说，无线网络面临的安全问题更为严重。在有线网络中，攻击者必须搭线接入到通信系统后才可以实施各种攻击，因此有线网络首先比无线网络多了一层物理安全保障。而在一个无线网络系统中，任何具有无线电波发射和接收能力的设备都能够很容易地从网络系统中窃听通信信息，也能够很容易地向网络系统中任意地发送信息。正是由于无线网络系统的这种“易读”、“易写”性，无线网络的安全问题呈现多样化：窃听、跟踪、篡改、阻塞、未授权的访问数据、完整性的威胁、拒绝服务、否认服务、未授权的访问服务等等，而且这些攻击都能够很容易地被攻击者实施。为了防止这些攻击，必须究其根源，从“易读易写性”这个弱点考虑解决节点认证和保密通信问题，这涉及节点间认证及密钥协商问题。认证及密钥协商是任何无线网络系统都必须解决的安全问题，也是无线 mesh 网络必须解决的关键问题之一。只有有效解决了认证及密钥协商问题，密钥管理以及安全路由协议才能得以实现。

笔者以车载 mesh 网络为研究背景，提出一种 mesh 网络的匿名接入认证方案。车载 mesh 网络和传统意义上的 VANET 极为类似，是一种特殊的 WMN，最初由 Naouel Ben Salem 等人[2]提出。在车载 mesh 中，车辆代替了传统意义上的 TAPs，道路两旁设有 WHSs，用户节点之间、用户和 WHSs 之间的认证和密钥协商问题非常重要，它是整个网络安全通信的基础。另外，用户身份信息和位置信息等隐私信息的保护在车载 mesh 网络中也很重要[8]。对于匿名性和隐私信息的保护，无论是有线还是无线，在国内外均有了一定的研究。文献[4]中的方案能有效保护节点的地理位置信息及用户隐私，抵御多种类型的主动和被动攻击，且具有可追踪性和匿名性，然而作者未考虑漫游情况以及协议的仿真；文献[5]中提出了一种邻居认证协议，它允许邻居节点在不揭示其身份的情况下进行彼此认证，然而需要对终点 ID(Destination ID)指出路径，只有条件匿名才能够到达目的地。文献[6]的方案能够实现合法用户的无条件匿名和非法用户的可追踪性，然而其计算开销较大。

基于以上相关研究背景，笔者借助于 Hash 函数和 Diffie-Hellman 算法来实现车载 mesh 网络中用户漫游时的匿名接入认证。在本文中，笔者将用户从一个城市进入另一个城市时视为漫游，每个城市的网络视为一个自治系统。

2 预备知识

2.1 杂凑函数(Hash)H

杂凑函数满足的条件[1]如下：

1)函数的输入是任意长，输出是固定长。

2)已知 x 求 $H(x)$ 较为容易，反之在计算上是不可行的。

3)对任意的 $x\neq y$，使 $H(x)=H(y)$ 在计算上是不可行的。

2.2 Diffie-Hellman 算法简述

设 p 是一个大素数，α 是 p 的本原根，p 和 α 作为公开的全程元素。用户 A 选择一个随机的保密整数 X_A，并将 $Y_A=a^{X_A} \bmod p$ 发送给用户 B。类似地，用户 B 选择一个保密的整数 X_B，并将 $Y_B=a^{X_B} \bmod p$ 发送给用户 A。然后 A 和 B 分别由 $k=Y_B^{X_A} \bmod p$ 和 $k=Y_A^{X_B}$ 计算出共享密钥。

3 无线 mesh 网络匿名认证和密钥协商协议

3.1 协议相关标识符说明

X_A^B：A 向 B 发送消息 X；

TID_A：实体 A 的临时身份标识；

ID_A：实体 A 的真实身份标识；

$E_k(X)$：用密钥 k 对消息 X 进行非对称加密；

(PK_A, SK_A)：A 的公、私钥对；

MC，MR，GW，TA：分别为 mesh 客户端、mesh 路由器、网关、可信中心。

3.2 漫游匿名认证协议

为叙述方便，现将整个网络具体抽象成图 1 所示的网络。假设 MC 所处的网络为 N_1，N_1 的临近网络为 N_2。现在 MC 即将漫游到 N_2。另外，假设各个网络内部的 GW 和 MR 之间相互信任。事实上，文献[3]中借助于 Diffie-Hellman 算法实现了 MR 和 MR 之间、MR 和 GW 之间的相互认证。当路由器之间、MR 和 GW 之间传送信息的时候，可以采用文献[3]中的方法进行相互认证，本文不再叙述。现假设各个路由器之间、MR 和 GW 之间相互信任，各个网络的网关可以由有线相连。

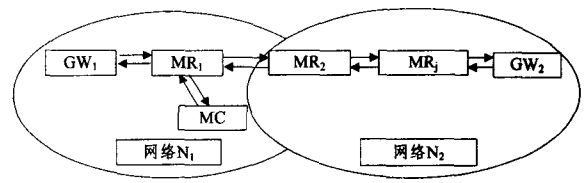

图 1 网络 N1 和 N2

整个协议的流程如图 2 所示，MR_1 和 GW_2 之间可能要经过几个 MR，在图中笔者用 MR_i 和虚线代表几个不同的路由器。以下笔者将具体阐述客户端认证和密钥协商的过程。

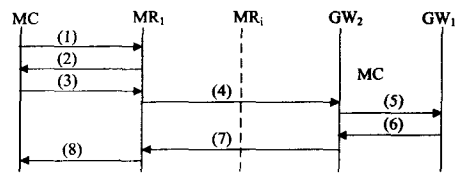

图 2 协议过程

图 2 中(1)—(8)分别为：

1)$\{C\}_{MC}^{MR_1}$

2)$\{E_{PK_{MC}}(C+1, T_1)\}_{MR_1}^{MC}$

3)$E_{PK_{MR_1}}\{\text{请求接入信息}, L_{MC}, T_2, C+2\}_{MC}^{MR_1}$

4)$\{ID_{N_1}, TID_{MR_1}, E_{PK_{N_1}}(L_{MC}||PK_{MC})\}_{MR_1}^{GW_2}$

5)$\{TID_{MR_1}, E_{PK_{N_1}}(T_{N_2}||L_{N_2}||E_{PK_{N_1}}(L_{MC}||PK_{MC})\}_{GW_2}^{GW_1}$

6)$\{E_{PK_{N_1}}(L_{MC}), E_{PK_{MR_1}}(E_{PK_{MC}}(L_{N_2})||ID_{N_2})\}_{GW_1}^{GW_2}$

7)$\{E_{MR_1}(PK_{MC}(L_{N_2})||ID_{N_2})\}_{GW_2}^{MR_1}$

8)$\{PK_{MC}(L_{N_2})\}_{MR_1}^{MC}$

以下将具体阐述协议的过程。

1)MC 向 MR_1 发送用 MR_1 的公钥加密的挑战信息 C，即 $\{C\}_{MC}^{MR_1}$。

2)MR_1 收到挑战信息后，用自己的私钥解密信息，并产生时间戳 T_1，用 MC 的公钥加密挑战信息 $C+1$ 和时间戳

T_1，然后将加密信息发送给 MC，即发送的信息为$\{E_{PK_{MC}}(C+1,T_1)\}_{MR_1}^{MC}$。

3) MC 收到信息后解密信息，确定 MR_1 合法后，便用路由器 MR_1 的公钥加密发送网络 N_2 的请求接入信息、T_2、L_{MC} 和 $C+2$，其中 $L_{MC}=a^x \bmod P$，x 为一随机大整数，p 是交管部门公开的大素数，α 为 p 的本原根，p 和 α 由交管部门公布。

4) MR_1 接到请求，解密信息，验证 MC 合法后便开始计算自己的假名 TID_{MR_1}，然后将自己的假名、网络的代理标识 ID_{N_1} 和 $E_{PK_{N_1}}(L_{MC}||PK_{MC})$一起发送给临近的路由器 MR_2，通过 MR_2 和其它路由器最终传到 GW_2。其中，L_{MC} 是 MC 的会话密钥生成信息，$TID_{MR_1}=H(ID_{MR_1})\oplus ID_{MR_1}\oplus ID_{N_1}$，其中"⊕"表示按比特异或运算，"||"为连接符。

5) GW_2 收到 MR_1 的访问请求后，用 N_1 的系统公钥加密 $T_{N_2}||E_{PK_{N_1}}(L_{MC}||PK_{MC})$，并连同 TID_{MR_1} 发送给 N_1，N_1 便可以验证 MC 和 MR_1 的身份。其中，T_{N_2} 是 N_2 产生的时间戳，L_{N_2} 是网络 N_2 的会话密钥生成信息，$L_{N_2}=a^y \bmod P$，其中 y 是 GW_2 随机选择的大整数。

6) 收到网络 N_2 发送来的消息后，GW_1 用网络 N_1 的私钥解密信息，并检查时间戳是否在有效期内。若时间戳失效，GW_1 会拒绝认证 MR_1 的身份，否则 GW_1 会计算 MR_1 的真实身份：$ID_{MR_1}=TID_{MR_1}\oplus H(ID_{N_1})\oplus ID_{N_1}$。

7) 收到 GW_1 发送的信息后，GW_2 对信息解密，得到 MC 的会话密钥生成信息，GW_2 将借助 Diffie-Hellman 算法计算会话密钥 $k=L_{MC}^x \bmod P$，并给 MR_1 发送消息：$E_{MR_1}(PK_{MC}(L_{N_2})||ID_{N_2})$。

8) MR_1 收到信息后，解密信息，并把 $PK_{MC}(L_{N_2})$发送给 MC。

最后，当 MC 收到 MR_1 发送的信息后，借助 Diffie-Hellman 算法计算会话协商密钥 $k=L_{N_2}^x \bmod P$，完成密钥协商，从而可以与网络 N_2 进行通信了。

4 协议分析

4.1 正确性和安全性分析

在整个客户端认证和密钥协商的过程中，消息的保密性由非对称加密算法保证，而消息的完整性由密钥 Hash 函数和 Diffie-Hellman 算法保证，密钥 k 的正确性和安全性是该协议的目标。以下给出部分定理，对协议的安全性进行说明。

定理 1 协议前向安全。

证明：第 3 节协议的计算安全性基于离散对数难题和安全单向函数。假设攻击者得到了 MC 或 GW_2 的私钥（甚至同时得到 MC 和 GW_2 的私钥），攻击者也难于获取 MC 和 GW_2 之间协商的旧会话密钥。因为会话密钥 $k=L_{N_2}^x \bmod P=L_{MC}^y \bmod P$ 中的 x 和 y 分别是 MC 和 GW_2 生成的随机数，它们并不直接在网络中传输，传输的是 L_{N_2} 和 L_{MC}。攻击者 A 很难由 L_{N_2} 和 L_{MC} 反推出 x 和 y，所以也就无法知道会话密钥，协议前向安全。

定理 2 协议可以防止假冒攻击。

证明：在会话密钥建立过程中，MC 和 MR_1，MR_1 和 GW_2，GW_2 和 GW_1 之间都对彼此之间的身份进行验证。MR_1 对 GW_1 的身份认证中，MR_1 和 GW_2，GW_2 和 GW_1 都用对方的公钥加密信息。这样，也就实现了相互之间的双向身份认证。攻击者若要假冒网络 N_2 的服务器，由于他没有信任的第三方颁发的私钥 SK_{GW_2} 而无法解密报文，也就无法冒充 GW_2 和 MC 协商共享密钥，因此这种攻击也是不可能的，从而可以防止假冒攻击。

定理 3 协议可以防止中间人攻击。

证明：攻击者也无法冒充 GW_2 与 MC 协商密钥，因为在协议中，只有 GW_1 向 GW_2 发送信息，GW_2 才能知道 MC 的协商密钥信息，而这一部分信息 GW_1 用 GW_2 的公钥加密，只有 GW_2 才拥有自己的私钥，得到 MC 的协商密钥信息，攻击者无法知道该密钥信息，因此无法和 MC 建立共享密钥 k。同样 GW_2 也不能和攻击者建立共享密钥 k，因此协议能防止中间人攻击。

定理 4 协议可以防止重放攻击。

证明：MR_1 使用了假名隐藏自己的身份，攻击者也无法得知 MR_1 的真实身份，可以保护 MR_1 的身份信息的隐私，从而也变相保护了 MC 的身份信息的隐私。另外，每次通信前选择了不同的随机数 x，y 计算会话密钥，有效地利用了时间戳，从而确保了密钥的新鲜性，有效地防止了重放攻击。

定理 5 协议具有一定的抗叛逆性和可追踪性。

证明：当合法用户在匿名接入的过程中，发送非法信息来扰乱路由，GW_1 可以在协议的第六步获得用户的身份信息，进而对其采取相应的惩罚措施。从而，本方案也具有一定的抗叛逆性和可追踪性。

4.2 性能和可行性分析

本文提出的 mesh 网络中用户节点漫游时的匿名认证和密钥协商协议采用了经典的 Hash 函数和 Diffie-Hellman 算法，用户节点所进行的运算仅仅是模素数运算和加密运算。和传统的公钥加密系统中的方案相比较，本方案降低了对用户节点的计算、存储能力的需求；与文献[6]中架构相比较，本方案大大降低了计算量，而安全性并不逊于文献[6]中的安全架构。虽然系统密钥管理的通信开销并没有降低，但是本方案的用户节点大多数是车辆，车上可以安装较强计算能力和存储能力的设备。一般情况下，车辆上电源的能量较充足，较少存在电池能量不足的问题，所以系统密钥管理的通信开销不会影响在现实中的应用。

本方案中用户节点 MC 的公/私钥可以在城市交管部门获得，各个城市网关服务器可以通过 Internet 相连接，网关服务器之间的数据传输是有线传输，可以认为是安全的，故本方案在现实应用中是可行的。

结束语 安全问题是影响 mesh 网络体系普及应用的主要问题，而认证是整个安全体系结构的基础。本文利用 Hash 函数和 Diffie-Hellman 算法，给出了一种高效的具有用户匿名性的漫游认证协议，并对协议的安全性、性能和可行性进行了分析。发现协议在一定程度上降低了用户节点的计算量和存储能力的需求，并且在现实应用中也是可行的。下一步将针对不同的敌手模型对本文的方案进行模拟，并针对更强大的敌手模型对方案进行改进，进一步提高其安全性和效率。

参 考 文 献

[1] 杨波. 现代密码学[M]. 北京：清华大学出版社，2003

[2] Salem B, Phubaux J. Securing Wireless Mesh Networks [J]. IEEE Wireless Communication, 2006, 13(2): 50-55

（下转第 81 页）

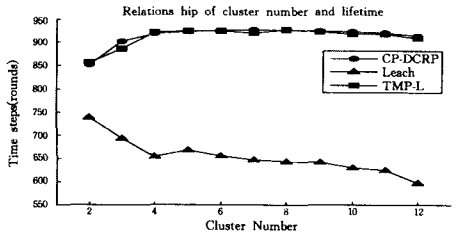

图 3　网络生命时间仿真

从图 3 可以发现，CP-DCRP 的网络生命时间要比 Leach 协议高出大约 50%，最高可达到 70%到 80%左右。同时 TMP-L 协议的网络生命时间基本上处于 CP-DCRP 协议的相同位置或者下面一点，说明 TMP-L 只根据当前剩余能量来选取 L 个簇头的机制没有 CP-DCRP 的基于预期剩余能量的预测机制优越。但是两者的网络生命时间几乎相当，都要远远高于 Leach，这说明两者的能耗均衡性能相当，都要远远好于 Leach。

4.4　节点能耗均衡性分析

定义网络节点能耗负载因子为第一个节点死亡时节点的剩余能量 $E_{residual}$ 与初始能量 E_{Init} 的比值：

$$load=\frac{E_{residual}}{E_{Init}} \tag{17}$$

网络节点平均能耗负载因子为：

$$load_{ave}=\frac{\sum_{i=1}^{N} load_i}{N} \tag{18}$$

其中，N 表示网络节点数目。

网络能耗均衡性可以用节点能耗负载因子的标准方差表示：

$$EBalanced=\sqrt{\frac{\sum_{i=1}^{N}(load_i-load_{ave})^2}{N}} \tag{19}$$

网络仿真环境与 4.3 节中的一样。下面仿真 Leach 协议和 CP-DCRP 协议网络的能耗均衡性能。为了显示方便，结果采用对数坐标。仿真结果如图 4 所示。

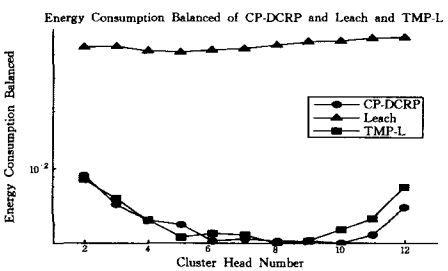

图 4　网络能耗均衡性能仿真结果

图 4 显示随着簇头数目的不断增加，Leach 协议网络的能耗均衡因子不断增加，节点之间的能耗越来越不均衡；CP-DCRP 与 TMP-L 协议的能耗均衡因子都非常小，并且十分接近，这是因为两种协议都是基于节点最大剩余能量的。Leach 协议的能耗均衡因子是 CP-DCRP 和 TMP-L 的 10 倍以上，CP-DCRP 和 TMP-L 要比 Leach 具有更好的能耗均衡性能。

结束语　CP-DCRP 协议基于节点的预期剩余能量，来预测接下来 L 轮的簇头节点。该协议具有很好的能耗均衡性能，最优簇头不受 L 的影响，同时当 L 增大时，网络平均每轮的能耗呈现下降的趋势。仿真结果显示 CP-DCRP 要比 Leach 具有更好的能耗均衡性能，网络生命时间大大延长。

参 考 文 献

[1] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Transactions on Wireless Communications, 2002, 1(4): 660-670

[2] 汪祥莉，李腊元，王文波. 无线传感器网络中的路由协议研究[J]. 计算机科学，2008，35(7)：50-60

[3] Jang Ki Young, Kim Kyung Tae, Youn Hee Yong. An Energy Efficient Routing Scheme for Wireless Sensor Networks[C]// International Conference on Computational Science and its Applications. Aug. 2007: 399-404

[4] Yang Haiming, Sikdar B. Optimal Cluster Head Selection in the Leach Architecture[C]// IEEE International Performance, Computing, and Communications Conference. April 2007: 93-100

[5] Bhuvaneswari P T V, Vaidehi V, Shanmugavel S. SPEAR: Sensor Protocol for Energy Aware Routing in Wireless Sensor Network[C]// Third International Conference on Wireless Communication and Sensor Networks. Dec. 2007: 74-78

[6] Satapathy S S, Sarma N. TREEPSI: Tree based Energy Efficient Protocol for Sensor Information[C]// IFIP International Conference on Wireless and Optical Communications Networks. 2006: 1-4

[7] Yuan Yong, Chen PMin, Kwon Taekyoung. A novel cluster-based cooperative MIMO scheme for multi-hop wireless sensor networks[J]. EURASIP Journal on Wireless Communications and Networking, 2006, 2006(2): 1-9

[8] Boukerche P, Cheng Xuzhen, Linus Joseph. A performance evaluation of a novel energy-aware data-centric routing algorithm in wireless sensor networks[J]. Wireless Networks, 2005, 11(5): 619-635

[9] Culpepper B J, Dung L. Melody Moh Design and Analysis Hybrid Indirect Transmissions (HIT) for Data Gathering in Wireless Micro-sensor Networks[J]. Mobile Computing and Communications Review, 2004, 8(1): 61-83

[10] Tan Huseyin Ozgur, Korpeoglu I. Power efficient data gathering and aggregation in wireless sensor networks[J]. ACM SIGMOD Record, 2003, 32(4)

(上接第 55 页)

[3] Islam S, Hamid A, et al. Preserving Identity Privacy in Wireless Mesh Networks[C]// Proceedings of International Conference on Information Networking. 2008

[4] 阮星华，徐敬东，于博洋. VANET 中位置路由协议的安全和隐私保护[J]. 计算机工程，2008，34(14)：166-170

[5] Zhang Y, Liu W, Luo W. Anonymous Communication in Mobile Ad Hoc Networks[C]// Proceedings of INFOCOM. 2005

[6] Sun J, Zhang C, Fang Y. A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks[C]// Proceedings of IEEE INFOCOM. 2008: 1687-1695

[7] 方旭明，马忠峰. 无线 mesh 网络的跨层设计理论与关键技术[J]. 西南交通大学学报，2005，40(6)：711-718

[8] Raya M, Hubaux J P. The Security of Vehicular Ad Hoc Networks[C]// Proceedings of SASN. 2005